WHAT IS CLAIMED IS

1. A security device log and reporting system for a data network, comprising:
a Log Collection unit, for collecting log files from security devices,
a Data Analysis and Log Archival unit for analysis and archival of log files,
and a Data and System Access Unit providing a user interface with the Data Analysis and Log Archival Unit.

2. A system according to claim 1 wherein the Log Collection unit comprises a Log Manager for managing log collection from a plurality of security devices.

3. A system according to claim 1 wherein the Log Collection Unit comprises a plurality of log collectors and a log collection manager for managing log collection from a plurality of log collectors.

4. A data network security management system for security device log archival and reporting comprising:
a log collection unit comprising a plurality of log collectors, each for collecting log files from a plurality of security device nodes and a log manager for collecting log files from the plurality of log collectors;
a data analysis and log archival unit for archival and automated analysis of log files transferred from the log manager,
and a data and system access unit providing a user interface to the Data Analysis and Log Archival Unit.

5. A system according to claim 4 wherein the log collection unit provides output to a storage manager and a Data Analysis manager, connected to a Data Analysis Store, of the Data Analysis and Log Archival unit, which also comprises a Archival unit associated with the Storage unit.

6. A system according to claim 4 wherein the user interface is a web based user interface

7. A system according to claim 1 wherein the data and system access unit wherein the user interface provides for log analysis summaries, trend analysis, controlled operational access and system configuration

8. A system according to claim 1 wherein the access unit comprises an authenticated, authorized, secured web based system.

9. A system according to claim 4 wherein the log collector receives logfiles from security devices comprising one or more device types comprising: Firewalls, CES, SPAM, FTP Drop Box and Anti-Virus.

10. A system according to claim 1 wherein the Log Manager LM interfaces with a Data Analysis Manager (DAM) and a Storage Manager (SM) and the LM comprises:
means for collecting logfiles from security devices,
means for pushing cached SD logfiles to a Storage manager for archival, and
means for providing log archival status updates to a Data Analysis Manager (DAM).

11. A Log Manager for a data network security management system, wherein the Log Manager LM interfaces with a Data Analysis Manager (DAM) and a Storage Manager (SM) and the LM comprises:

means for collecting logfiles from security devices, means for pushing cached SD logfiles to a Storage manager for archival, and means for providing log archival status updates to a Data Analysis Manager (DAM).

12. A system according to claim 1 wherein the Log Collector Manager (LCM) interfaces with a Data Analysis Manager (DAM) and a Storage Manager)SM) and the LCM comprises:

means for receiving logfiles from the plurality of log collectors,

means for obtaining a logging system configuration from the DAM,

means for propagating the configuration to individual LC associated with Security devices,

means for providing notification to the LC to begin transfer of SD log files, and

means for pushing cached SD log files to the Storage manager for archival, and

means for providing log archival status updates to the DAM.

13. A system according to claim 1 wherein the Data Analysis and Log Archival unit comprises a Storage Manager (SM) and a Data Analysis Manager (DAM) and the SM comprises

means to receive security device logs from the Log Collector Manager,
means for system archival,
means for management of online and offline log archivals and transition of logs form online to offline status,
means to provide the Data Analysis Manager (DAM) with access to SD logs on request, and
means to provide the DAM with access to the SM log Archival tables on request.

14. A security device log and reporting system wherein archival of log files is separated from analysis of logfiles.

15. A security device log and reporting system comprising a Log Manager, the Log Manager having a distributed interface for receiving logfiles from a plurality of security devices, and is the interface to a Data Analysis and Archival unit of the system.

16. A security device log and reporting system according to claim 15 wherein the Log manager comprises an intermediary caching system for log files received from the plurality of security devices.

17. A security device log and reporting system according to claim 14 comprising an Data Analysis and Archival Unit, a Log Collection Unit comprising a Log Manager, and Data and system Access Unit, wherein Data Analysis and Archival Unit interfaces with only a Log Manager and a Data and System Access Unit, whereby interfaces are easily protected via a firewall and instrusion detection system.

18. A method of managing security device log archival and reporting for a data network security , comprising

collecting log files from a security device node at a log collector

collecting log files from a plurality of log collectors at a log collection manager

transferring log files from the log collection manager to a data analysis and log archival unit for archival and analysis.

19. A method of managing security device log archival and reporting for a data network security , comprising

collecting log files from a security device node at a log collector

collecting log files from a plurality of log collectors at a log collection manager

transferring log files from the log collection manager to a data analysis and log archival unit for archival and analysis, logfile analysis being separated from log file archival.

20 A method according to 18 comprising providing user access to the Data analysis and log archival unit via a a data and system access unit.

21. A Storage Manager for a security device log archival and reporting system comprising means for receiving security device logs from the log collector manager for system archival,

means for management of online and offline log archival and transition of logs from online to offline status,

means for providing the DAM with access to security device logs on request,
means for providing the DAM with access to the SM log archival tables on request.

22. A storage manager according to claim 21 comprising means for differentiating types of log files.

23. A computer readable medium for implementing a method of managing security device log archival and reporting for a data network security , comprising

collecting log files from a security device node at a log collector

collecting log files from a plurality of log collectors at a log collection manager

transferring log files from the log collection manager to a data analysis and log archival unit for archival and analysis.

24. A method of managing security device log archival and reporting for a data network security , comprising

collecting log files from a security device node at a log collector

collecting log files from a plurality of log collectors at a log collection manager

transferring log files from the log collection manager to a data analysis and log archival unit for archival and analysis, logfile analysis being performed independently from log file archival.